EXHIBIT 10

MAO DECLARATION
ISO PLAINTIFFS'
MOTION FOR CLASS CERTIFICATION

DOCUMENT SOUGHT TO BE SEALED

Google

GEO Privacy Champion

Key Privacy Concepts

Privileged & Confidential

Agenda

- Data Classification
- Transparency & Control principles
- Data Protection
- Wipeout
- Logging

Google

Privileged & Confidential

Data Classification

Useful links:
go/dcg

Google

Privileged & Confidential
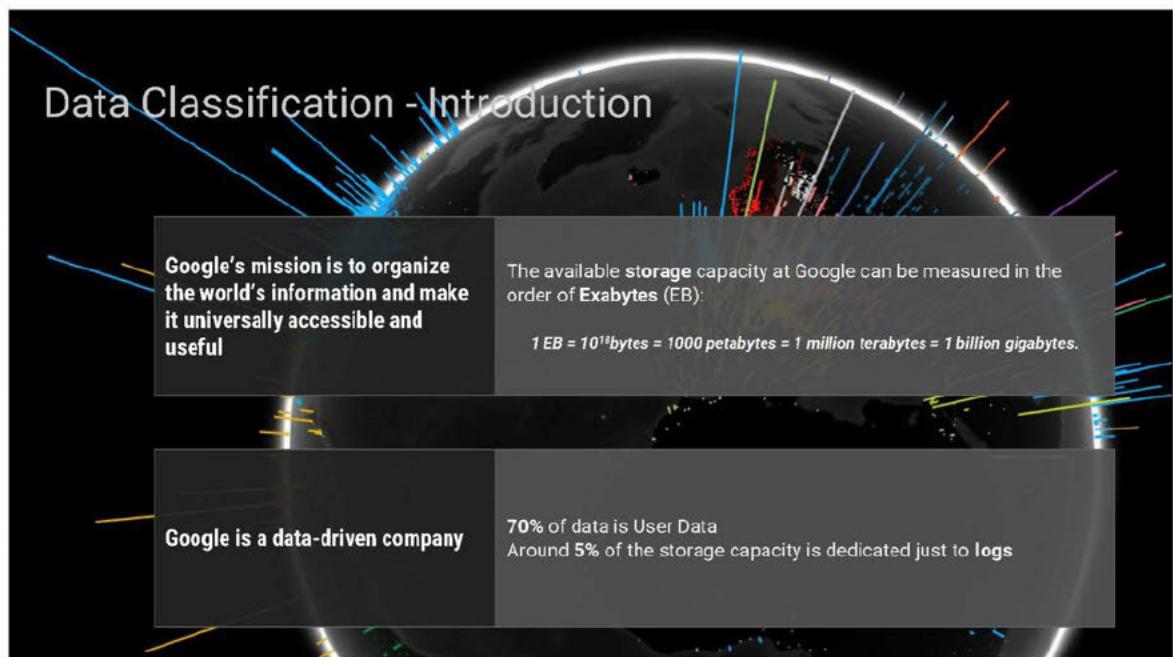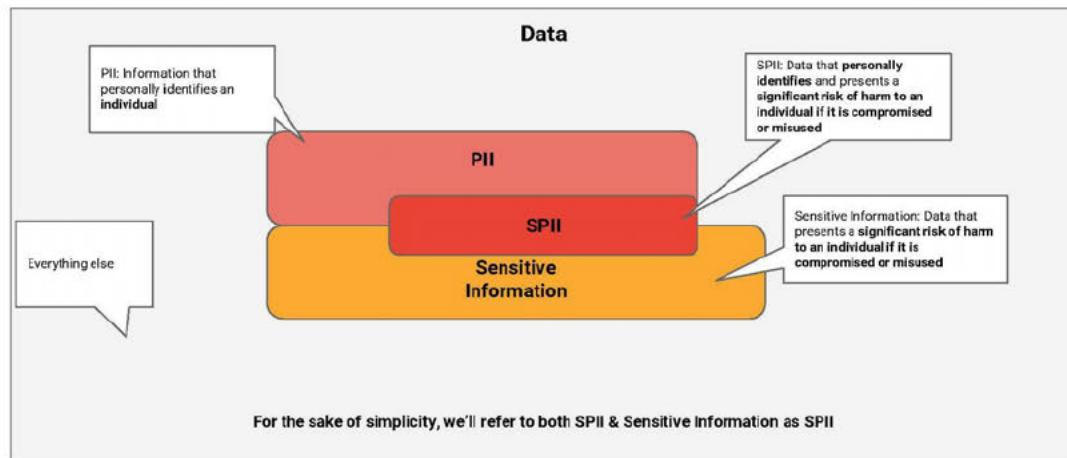
Data Classification Guidelines: go/dcg

2 slide

PII - Personally Identifiable Information

PII: Information that personally identifies an individual and any other data which can be reasonably linked to such information by Google. Examples:

- An individual's name, email address, mailing address, or telephone number, either alone or in combination, are considered PII.
- PII includes any information that is combined with PII or can be linked to PII with a reasonable level of confidence based on information available to Google.
- Solely for the purposes of classifying data internally at Google, the following types of data are classified as PII by default until reclassified: IP addresses, and unique account identifiers (such as account or customer ID, GAIA ID, or screen name).

Data categorized as PII under these Guidelines may differ from data defined as "personal information," "personal data," or "personally identifiable information" in Google's external statements or applicable laws.

Google

Privileged & Confidential

SPII - Sensitive Personally Identifiable Information

SPII: Data that presents a significant risk of harm to an individual if it is compromised or misused. Examples:

- *Account Credentials:* non-public information used to log in, authenticate or authorize activity as a particular individual
- *Government Identification Numbers:* any state or national identification number, including Social Security Number (SSN), passport number, or driver's license number
- *Cardholder Data (CHD):* Information associated with a specific payment card account (including credit cards, debit cards, or any other payment card)
- *Financial Account Data:* Information about a specific financial transaction (financial account numbers, amount of the transaction, what was purchased, the identity of the merchant, and the date of the transaction)
- *Healthcare Information:* details about an individual's past, present or future physical or mental health or condition.
- *Sensitive Background Information:* any information relating to an identifiable individual's ethnicity, political affiliation, sexual orientation, or religious affiliation.

Data categorized as SPII may differ from data defined as "sensitive personal data" in Google's external statements or applicable laws.

**Google**   Privileged & Confidential

SPII - Sensitive Personally Identifiable Information

SPII: Data that presents a significant risk of harm to an individual if it is compromised or misused. Examples:

- *Account Credentials:* non-public information used to log in, authenticate or authorize activity as a particular individual
- *Government Identification Numbers:* any state or national identification number, including Social Security Number (SSN), passport number, or driver's license number
- *Cardholder Data (CHD):* Information **Sensitive and Personally Identifiable** count (including credit cards, debit cards, or any other payment card)
- *Financial Account Data:* Information about a specific financial transaction (financial account numbers, amount of the transaction, what was purchased, the identity of the merchant, and the date of the transaction)
- *Healthcare Information:* details about an individual's past, present or future physical or mental health or condition.
- *Sensitive Background Infor* **Sensitive but not necessarily Personally Identifiable** hnicity, political affiliation, sexual orientation, or religious affiliation.

As anticipated, let's refer to both these classes as SPII

Google   Privileged & Confidential
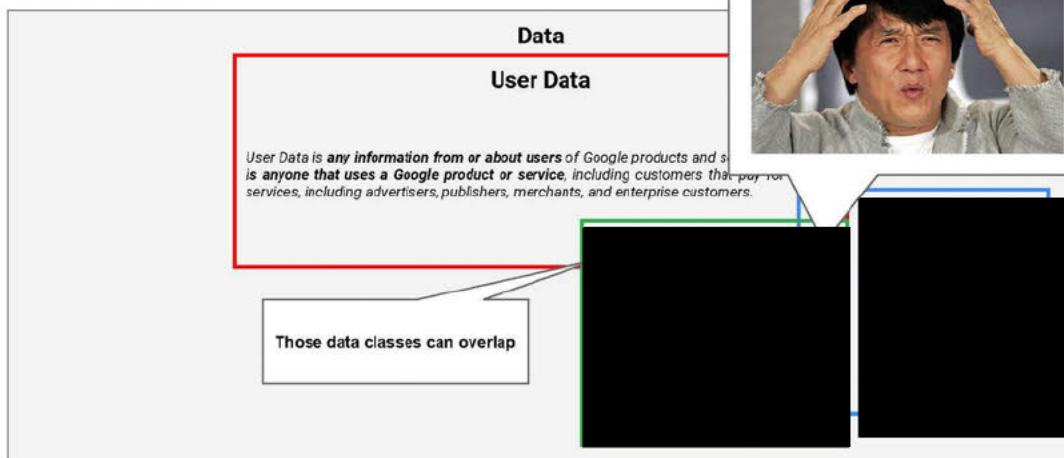
Data Classification Guidelines: go/dcg

Google's corporate services are intended for use with Google's data, and all data transmitted or stored using corporate services will be treated as the property of Google, even if the data turns out to be for personal rather than work-related purposes .... Googlers may use corporate services for personal purposes within reason, but any expectations of privacy when doing so are diminished ...

Data Classification Guidelines: go/dcg

2 slide

animazione
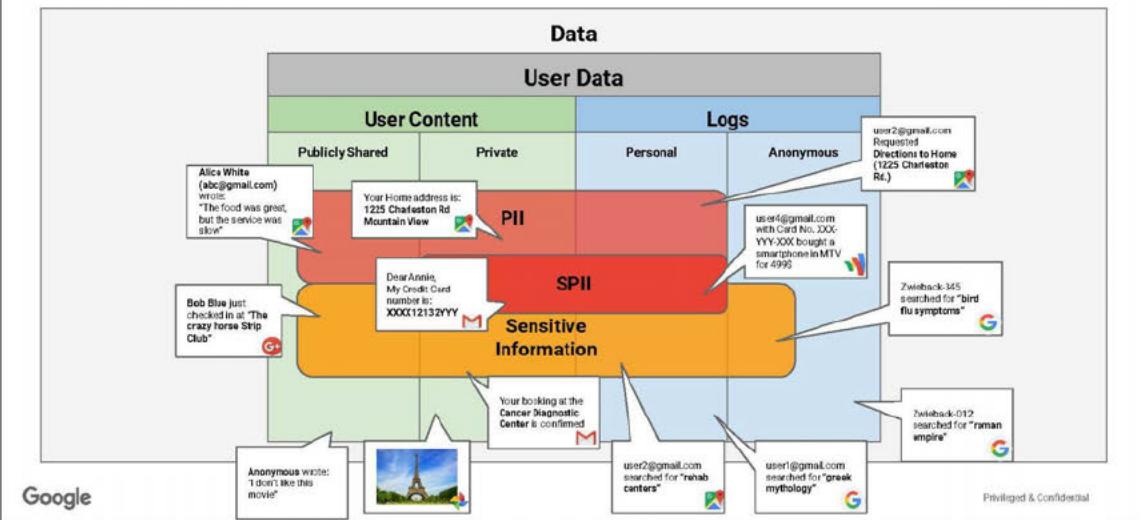
Data Classification - Access Levels

At Google, 3 different access levels exist:

			Confidential
Public	**Need-To-Know**		any information that Google has an **obligation** or a need to **keep private**, including data that Google owns, as well as data that Google receives from others.
information is information that has been **intentionally** and **explicitly** made available by Google* **to the public**. (*) by the user, in case of user data.	information associated with **serious legal, privacy or business concerns**. Information is properly classified as Need-To-Know whenever it would cause a significant risk of harm if it were used or disclosed improperly.		
No information at Google is Public by default.	Need-To-Know information is **shared only with authorized individuals** for a **specific purpose**.		Confidential information is **only shared with Googlers** and those **third parties** we work with **who have agreed in writing to keep the information private**.

Google

Privileged & Confidential

Anonymization

Google   Privileged & Confidential

Transparency & Control

Useful links:
go/udc

Google

Privileged & Confidential

Introduction to Transparency & Control

All products that opt-in users into data collection, should provide users with:

- **Transparency**: ability to see / manage the collected data
- **Control**: ability to opt-out of data collection

Google   Privileged & Confidential

User Data Transparency and Control

Transparency involves clear, comprehensive communication from Google to the user. It means **users are never surprised** by the collection, use or retention of their data.

- **What:** A clear explanation of any consequential change to the availability or presentation of user data.
  - e.g. privacy-related user setting or sharing actions.
- **Where** the user expects it. Obvious, non-intrusive.
  - e.g. in-flow on a dialog or settings page.
- **When** the user needs it and can use it.
  - **Before** the any action is taken, even if reversible.
- **How** the user can best understand it.
  - Friendly, understandable language. Links to more detailed information.

Google

Privileged & Confidential

Googlers aren't typical users. It's kind of a cliche, but it's even more relevant to T&C than it is to dogfood feedback. We can't practically aim for "no single user will ever be surprised", but this absolutely needs to be true at the high end of the distribution.

Example of a "When" transparency problem (courtesy of Bryan Horling in a comment thread on Geo Footprints, Technical Options)
We push for real-time wherever possible because 1) people are more aware of an event right after they do it and 2) we never want to make it look like we don't have data that we have.

When data arrives late, then users can look for that activity, and incorrectly conclude that the data was not recorded, only to be surprised by it at some later date.

This undermines our broader story on transparency and control. To put this in a different perspective, there are also European DPAs who are actively testing our products and requesting written explanations of their findings, to see what data shows up when and how deletion requests affect what we store. They influence policy, regulation and litigation, so it's good to have a tight, coherent story.

So implementing proper T&C sound kind of tricky, no? Fortunately, we have a framework to help with most of it. .... Footprints (next slide)

Setting the expectations

We're not expecting each new piece of data we collect to have its dedicated switches, knobs and transparency UI - most of the times it falls within the boundaries of one of the existing UDC (User Data Controls) settings, and we can leverage existing tools:

- **Web & App Activity (WAA)**
- **Supplemental Web & App Activity (sWAA)**
- **Voice & Audio Activity (VAA)**
- **Device Information (DI)**
- **Location History (LH)**
- **YouTube Search/Watch History (YTS/YTW)**

Google

Privileged & Confidential
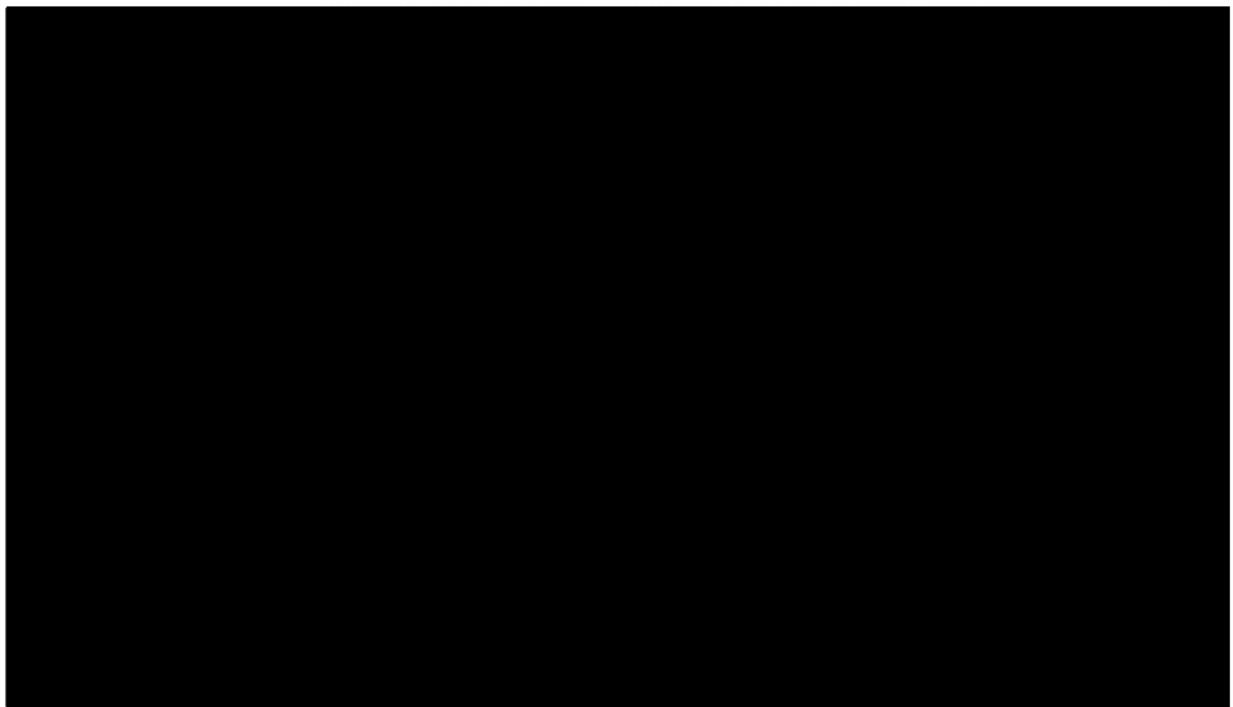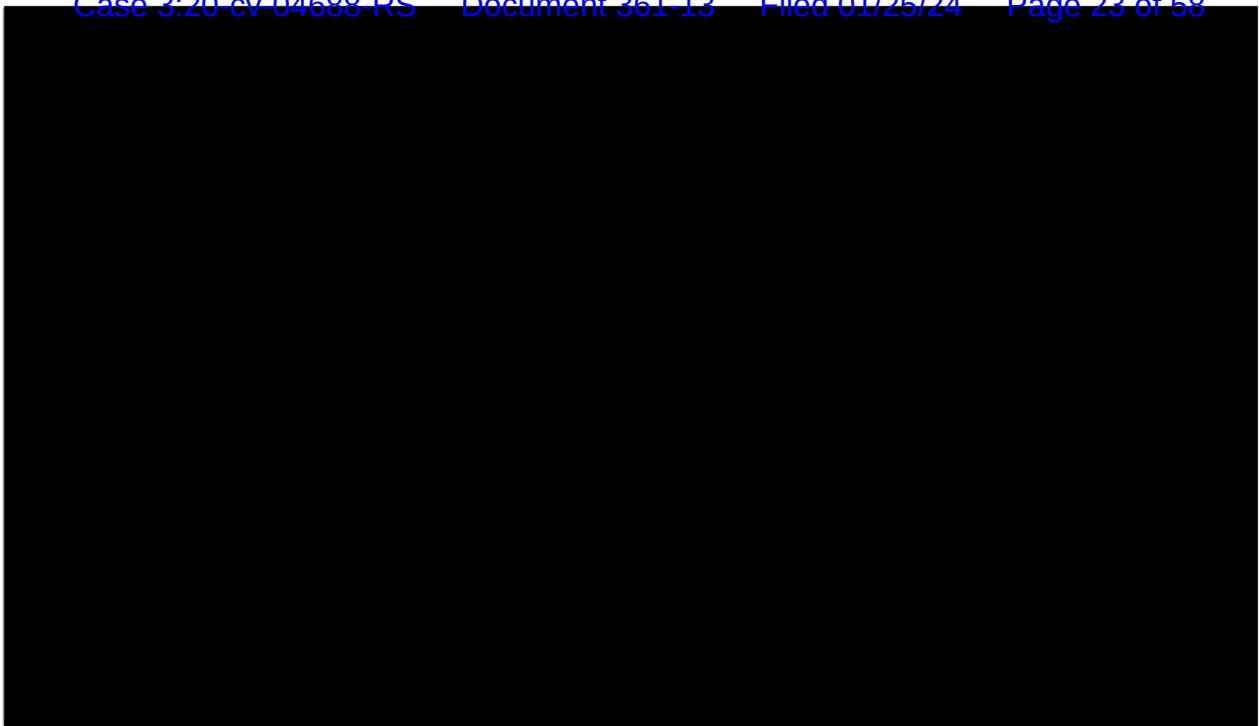
Example: Location History vs Web & App Activity

Both controls allow to log user data based on the condition that we make use of it and provide users with Transparency & Control, but:

Web & App Activity
Save your search activity on apps and in browsers to make searches faster and get customized experiences in Search, Maps, Now, and other Google products.

Store data (e.g.: query & context) as a consequence of explicit user actions. Location is part of the context for such actions.

Transactional Location data

Location History
Creates a private map of where you go with your signed-in devices in order to provide improved map searches, commute routes, and more.

Continuously store location data in background

Background Location data

Google

Confidential + Proprietary

Identifying bad ideas...

Understanding these principles helps us understand WHY some ideas are bad, because **acting on intuition is not always best**. What are the principles being applied by the Geo Privacy Champion below?

> Let's log phone unlock events along with location data... and then we provide transparency through Web & App Activity

> Not so fast! The **user would get insufficient value** out of "Unlocked your phone at $place" events. And even though unlocking is an "explicit action" it is also unavoidable. Further, this data **is no better than collecting location data periodically**, and we already have Location History for that.

Use information to provide our users with valuable products and services.
FAIL! Dozens of events like "You unlocked your phone near 4th and main" are of dubious value in isolation, and offers **no additional value** beyond location history which we already have.

Give users meaningful choices to protect their privacy.
FAIL! Allowing the user to "choose" not to use the product is **not a meaningful choice**. Asserting otherwise risks being made into the subject of your very own meme template!

Google   Privileged & Confidential

Try to make somebody given an answer to "which principles are being applied here?".

Post-transition:
Can anyone guess the target of that link?
It's Vic Gundotra.

Who's he?
Former SVP of social.

Why's he relevant?
During the real names privacy hoopla, he publicly proposed giving users the "choice" not to use the product if they don't find it's privacy controls sufficient. Guess where he is now? He resigned. (do provide the context: that fact isn't necessarily directly related to the meme content, but it's still relevant as it shows that even high-level pressure against these principles can be successfully opposed.)

A word on T&C for "Share" action (go/core-sharing-tenets)

1. Users have to know what *identity* is sharing. (**Who am I?**)
2. Users have to know what *content* they are sharing. (**What am I doing?**)
3. Users have to know what *audience* they are sharing to. (**Who can see?**)
4. Users must have access to a "make it stop" button. (**How can I stop this?**)

Why? Because this is the subject matter of our consent decree, it's one of the most sensitive things which it's possible to do at Google.

Google

Privileged & Confidential

Data Protection

Useful links:
go/confidential
go/dpp

Google

Privileged & Confidential

Data Protection - Introduction

Data Classification and Access Levels would be just a fancy exercise without effective **protection measures**. Data Protection is not just about encryption: in its widest sense it is about enforcing:

	Confidentiality	information is **not made available or disclosed to unauthorized** individuals, entities, or processes
	Integrity	the **accuracy** and **completeness** of data are **maintained and assured** over its entire lifecycle
	Availability	data is **accessible and usable when needed** by an authorized entity

From a **Privacy** standpoint, we **focus** mainly on those two aspects

Google

Privileged & Confidential

GOOG-RDGZ-00161391

Data Protection Technologies - Overview
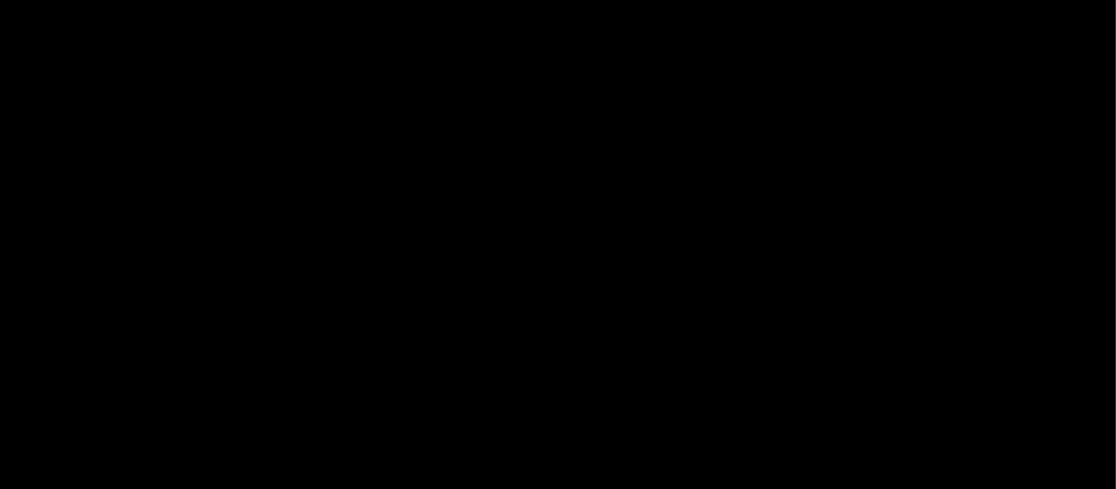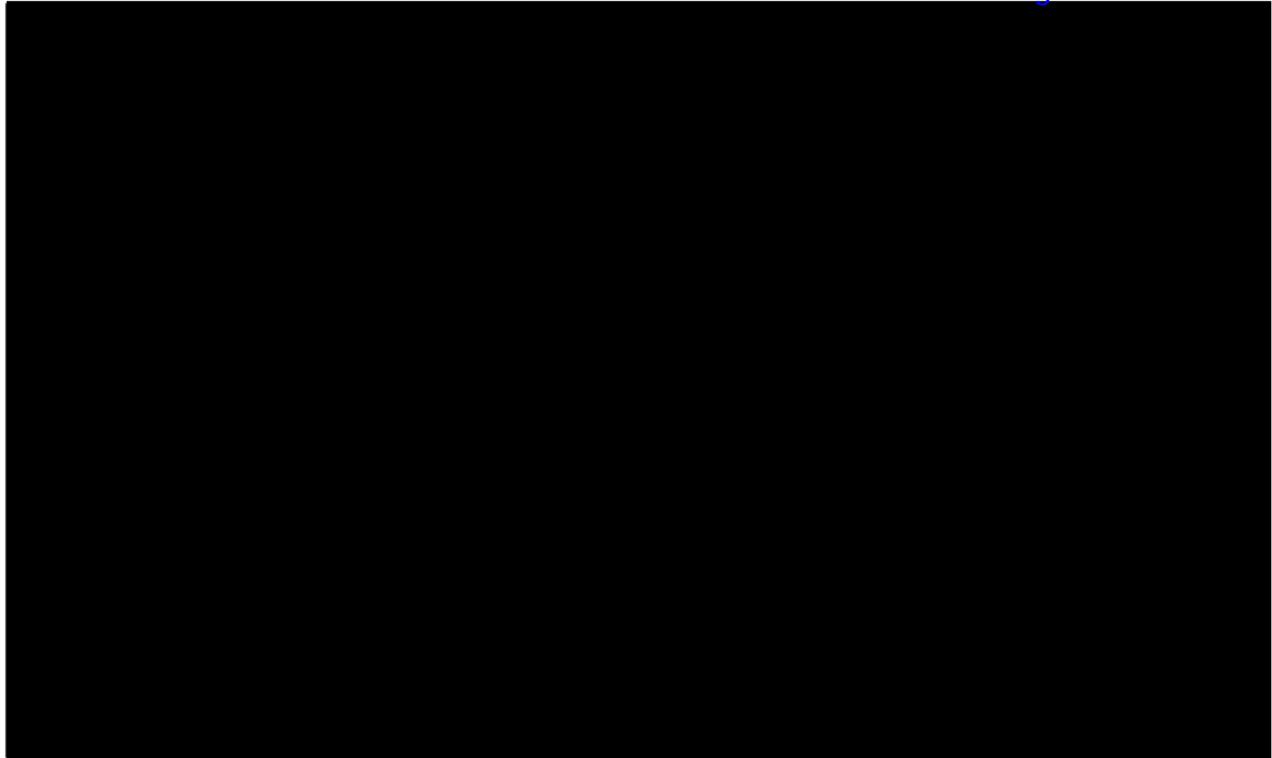
Auditing

Authentication and Authorization are at the core of the data protection stack, however ignoring what happens after the authentication would seriously undermine the effectiveness of the entire stack, exposing data to abuse or misuse.

At high level, User Data can be accessed in two ways:

- **Directly,** ███████████████████
- **Indirectly,** ████████████████

Both of them need auditing, though with different tools and methods.

Google

Privileged & Confidential

Auting Googlers –
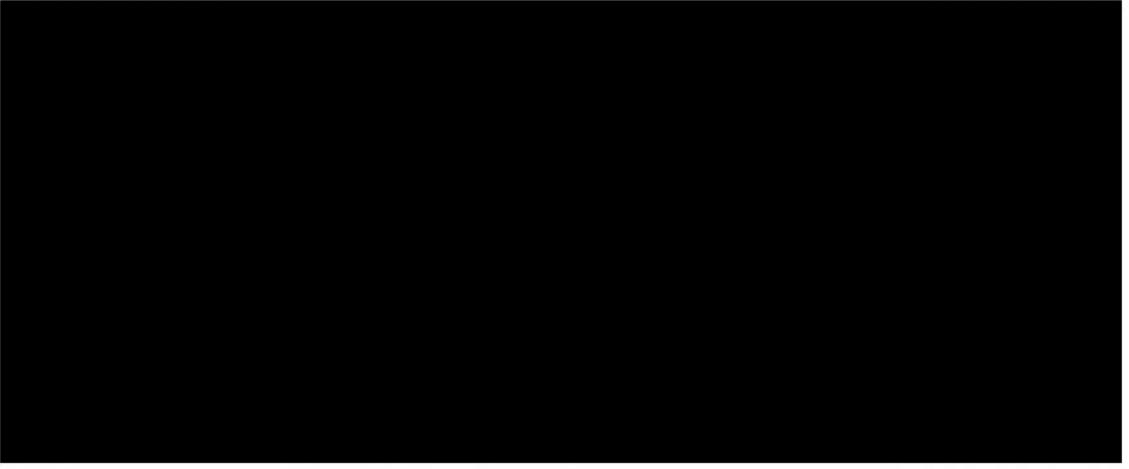
Google

Privileged & Confidential

go/gin
go/UDAAG
ginui/
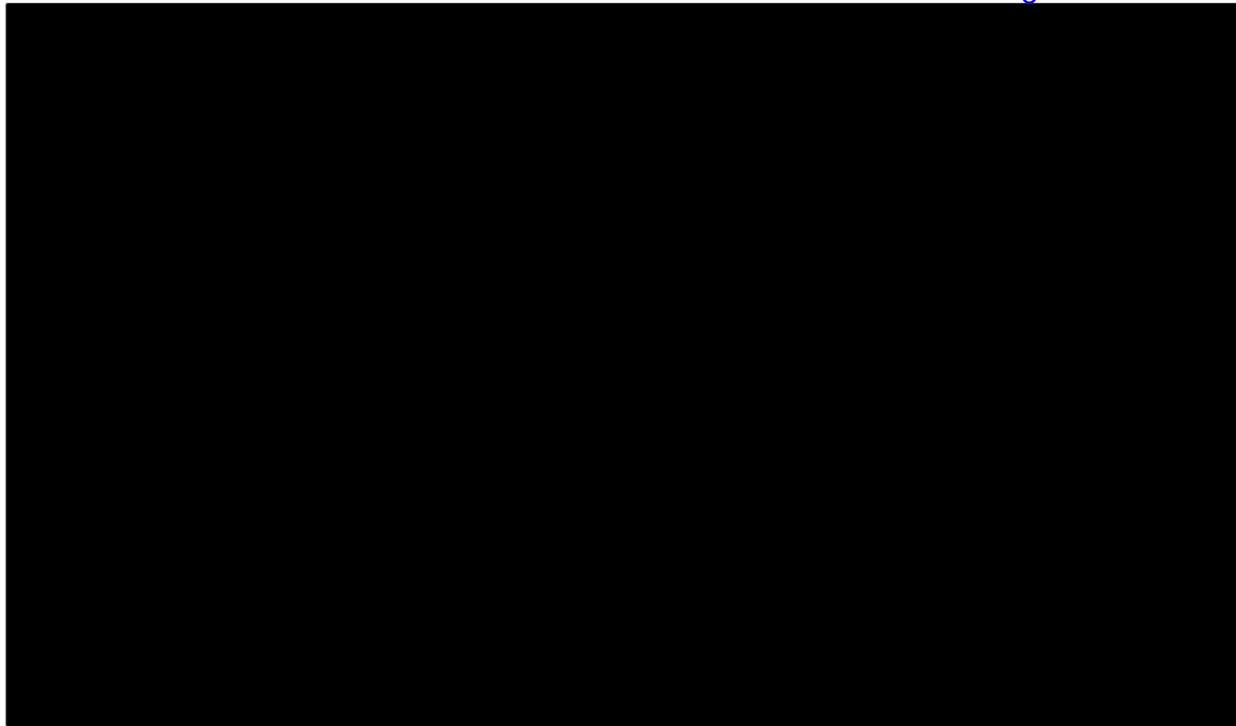
go/bcid
bcid/

Encryption (and not only) - ███████

████████████████████████████████
████████████████████████████████
████████████████████████████████
████████████████████████████████
████████████████████████████████
████████████████████████████████
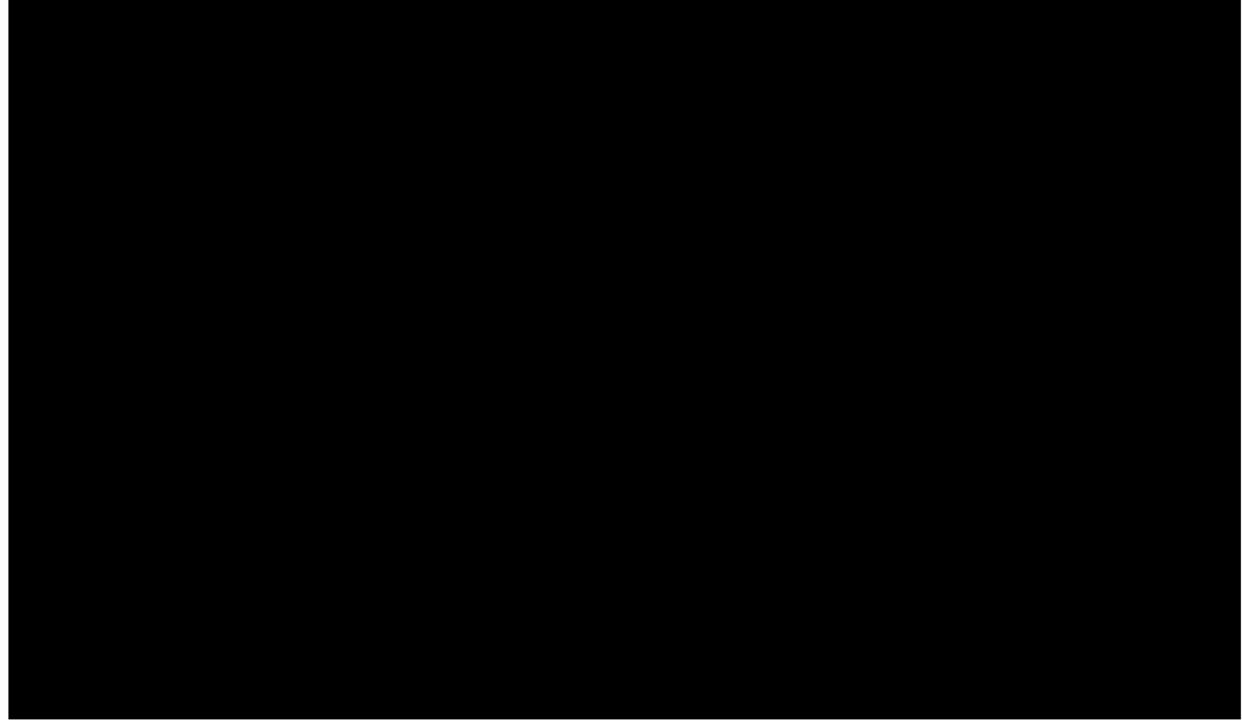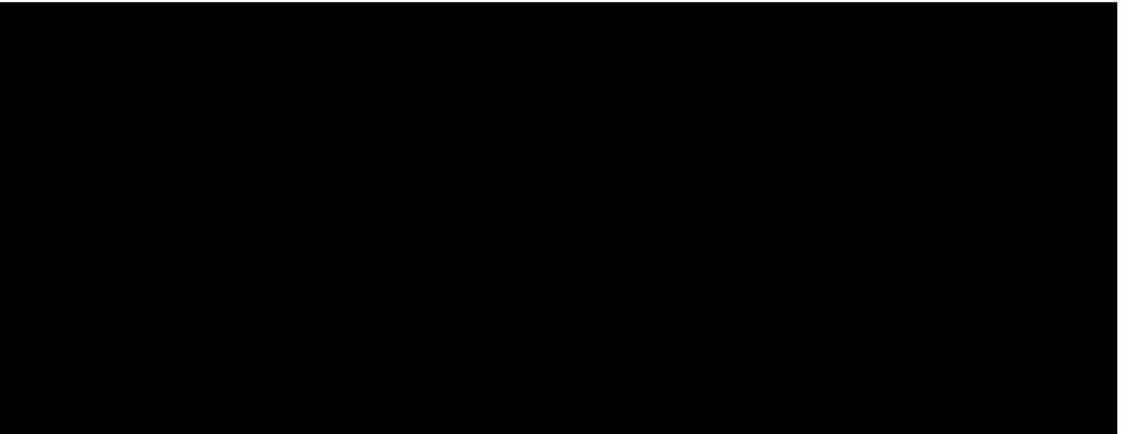
Google   Privileged & Confidential

go/estorage

██████████████████████

Wipeout - Introduction

In the good old times, most databases and storage systems offered **granular CRUD (Create, Read, Update, Delete) methods**. However in the last few years the **Delete,** which possibly is the most complex and less used one, has been sacrificed on the altar of performance and scalability.

In highly distributed, high performance storage systems, **"deleting" is either simplistic (e.g.: "tombstoning" the data), or costly (e.g.: copying the entire dataset, minus the records to delete).**

Plus, **data is the gold of the 21st century.**

Really Deleting Data is HARD

████████████████, which only offers SELECT and MATERIALIZE primitives.

Wipeout

The goal of **Wipeout** is to provide **transparency around user data deletion**: it is the verification mechanism that ensures we **honor service removal and account closure requests from users within a reasonable timeframe**.

In this context a "reasonable" amount of time is **63 days*** from the time of the user request action **for live systems** and **180 days** from the time of the request for offline/backup systems. Unless an alternative retention plan has been defined and approved.

Wipeout Events

- **service removal** - a service is disassociated with an account (e.g., removing Google+), but the account still exists.
- **account closure** - an account, and all its associated data, is terminated by user request.
- **item deletion**** - a single item (e.g.: a photo or a day of Location History) is explicitly deleted by the user.

(*) intended as the request-to-physical deletion time (depends on storage)
(**) **item deletions** are not monitored by the Wipeout dashboard.

Google

Wipeout team t-shirt with team logo

FRONT   BACK
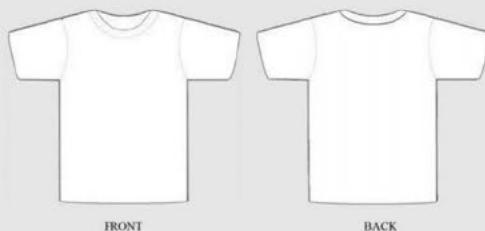
Sold at every store near you!

Privileged & Confidential

To be Wipeout compliant, products must:
Delete live user data within 63 days of a deletion request.
Delete all user data within 180 days of a deletion request.
Integrate with the Wipeout Dashboard.
Maintain an updated Privacy Design Document.
Designate an owner to respond promptly to Wipeout dashboard alerts.

Pubsub - no cleanup

aschou

We have to delete a lot of data.

- Any data collected or processed from (or about) users.
  - Any data which is keyed to a particular user identity;
  - Data derived from identity-keyed data;
  - Per-user aggregates and pseudonymous data;
  - Some metadata
- But we sometimes can (or have to) keep:
  - Genuinely anonymous or aggregated data;
  - Billing or payment data;
  - Data which is requested as part of some ongoing legal investigation;

Google

Privileged & Confidential

(Backup copies of data which we have in another form. (?)

It isn't always obvious where the data lives.

- Data which is keyed to a non-GAIA identifier:
  - Zwieback
  - MAC Address, Android ID, Apple ID
  - Email address, Phone Number
- Data stored in someone else's row:
  - ACLs pointing at someone else's data;
  - Recommendation data;
- Data which contains an implicit identifier or is traceable to a user identifier:
  - Obfuscated GAIA
  - Anything with enough persistent bits to create an implicit identifier

Google

Privileged & Confidential

Even when we know where it is, it's still hard.

- Distributed architecture:
    - Within a single datastore, data may have multiple replicas;
    - Eventual consistency makes deletion timing difficult;
- Massive Scale, Zero-Tolerance Guarantees:
    - Deletions must either commit or noisily fail.
    - An issue affecting 1 in 1,000,000 users per year affects 2,000 users.
- Deep tech stack:
    - Data is constantly in transit.
    - Deleting in one datastore does not necessarily get rid of particular data.

Google   Privileged & Confidential

GOOG-RDGZ-00161405

We have a lot of infrastructure to deal with it.

Google

Privileged & Confidential

But things still fail.

- People think their storage handles it automatically… and it doesn't.
- People think the data in their system is fresh… and it isn't.
- People think their online deletion path is reliable… and it's only *mostly* reliable.
- People think that deletion is globally instantaneous… and the speed of light is finite.
- People try to anonymize… and fail.

Google

Privileged & Confidential

Sometimes 'fresh' is actually from a different origin datastore

Logging

Useful links:
go/justice-league
go/▮▮▮▮
go/datapol-gdh

Google

Privileged & Confidential

(*) users need to have transparency about the presence of precise location data attached to events
(**) aliases and corresponding addresses must not appear together in the "query" field
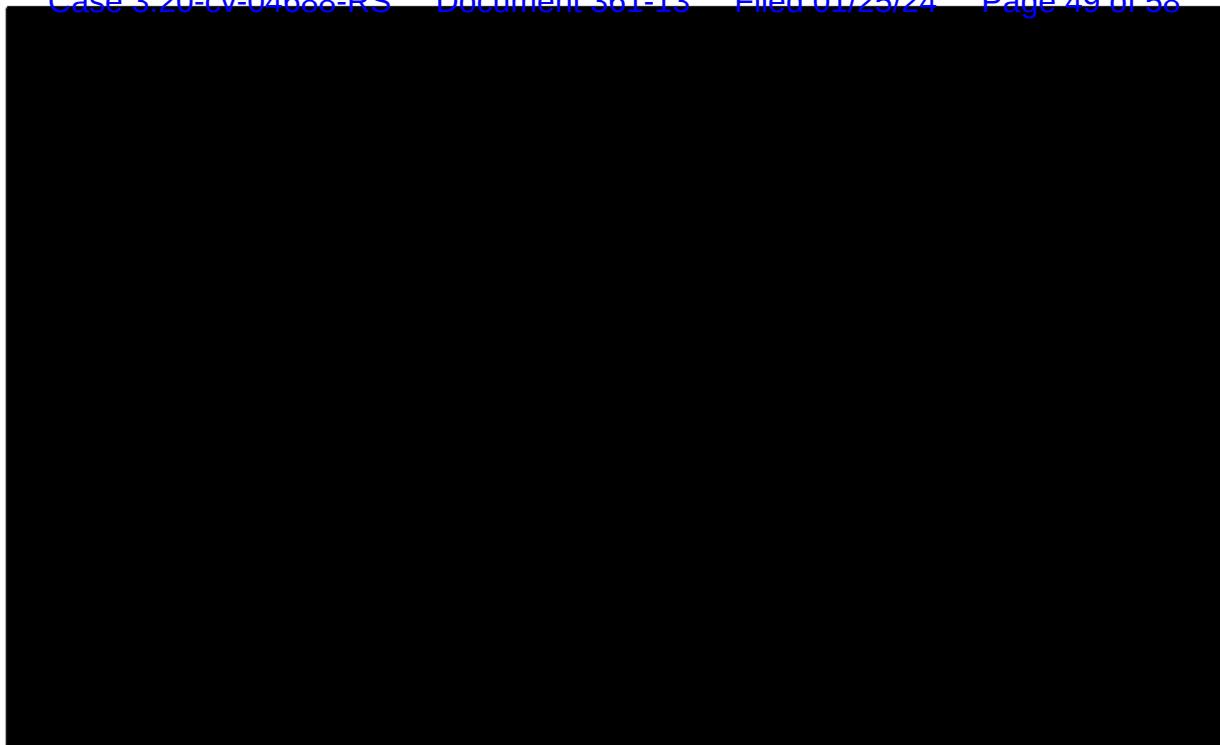
Datapol Annotations

The **Google Data Policy (DataPol) protocol buffer annotations** provide a systematic way of **specifying the intended semantics of user data**. This allows Google to identify and control this data and to help applications handle a user's data in ways that comply with Google's privacy policies. **These annotations are used in a wide range of privacy tools and processes, such as policy checking, privacy analysis, access control, and privacy documentation.**

What needs to be annotated

- SPII
- PII
- Pseudonymous IDs, session IDs or timestamps that can be used to join records from multiple sources.
- Cookies, document IDs, user agents, URLs, HTTP headers, and requests.
- IP addresses, and device IDs.
- Location of the user or a device.
- Demographic information such as birth date, age, or gender.

... and this is how do they look like...

```
optional string business_address = 800 [
    (datapol.semantic_type) = ST_LOCATION,
    (datapol.location_qualifier) = {
        precise_location: true
        non_user_location: true }];
```

Google

Privileged & Confidential

Logs Access Types

Users that need to access Logs, are assigned a specific **Logs Access Type** based on their needs. Each level grants access to a specific set of fields. The set of fields that each level is allowed to access, is identified through **Datapol Annotations**.

The [REDACTED]

Google

Q&A

Google

Privileged & Confidential

Appendix

Google

Privileged & Confidential

GOOG-RDGZ-00161418
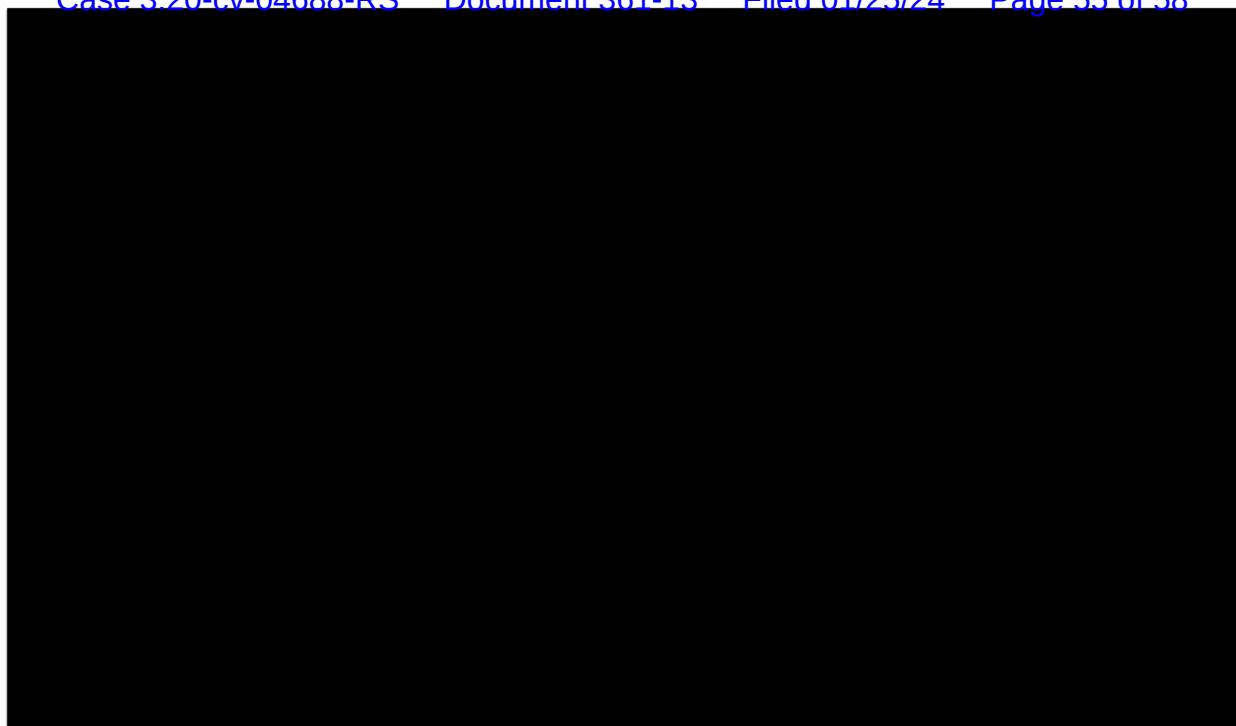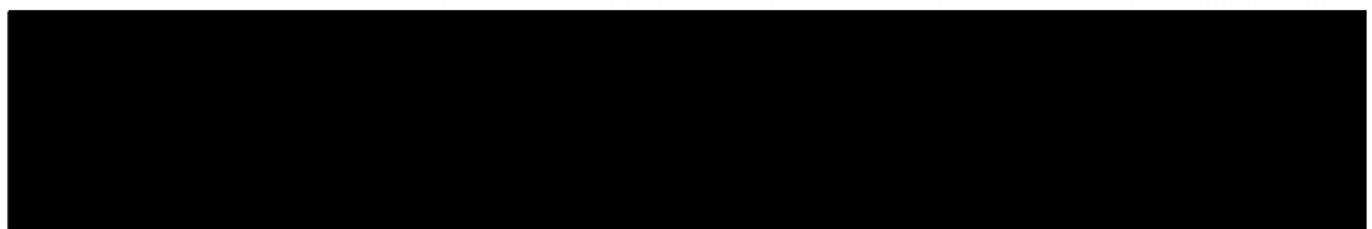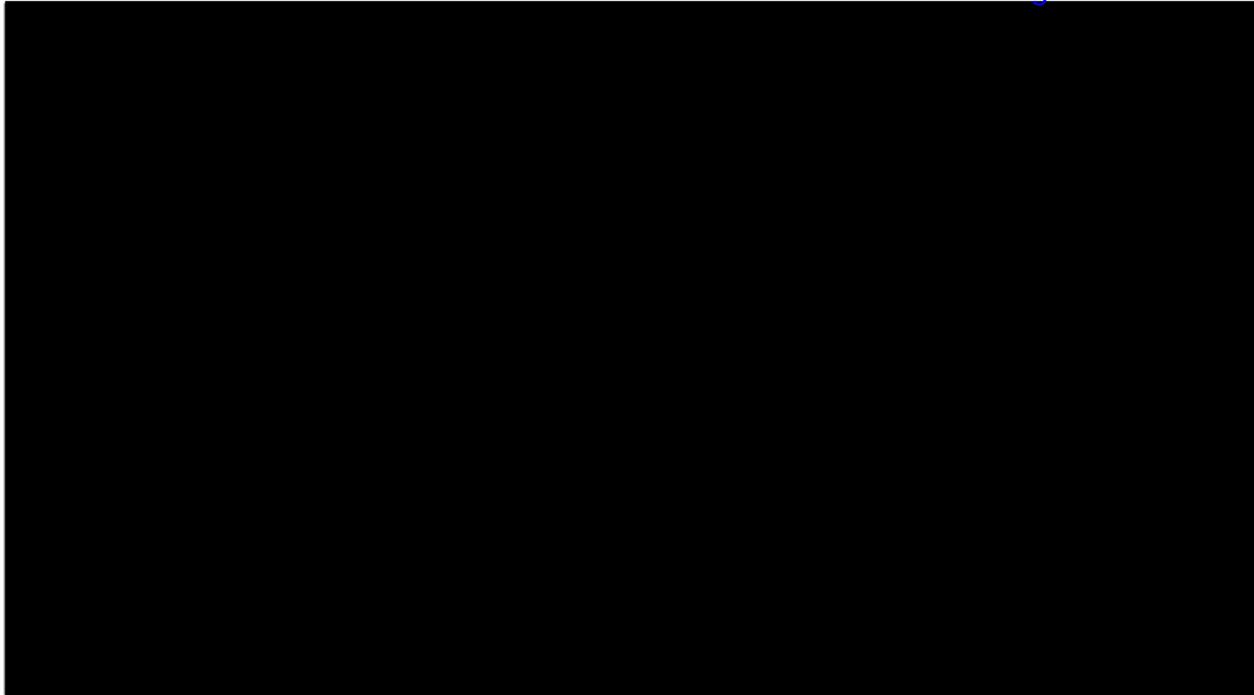
Encryption (and not only) - Introduction

Google   Privileged & Confidential

go/estorage